YÖNETMELİK

Bankacılık Düzenleme ve Denetleme Kurumundan:

BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ BAĞIMSIZ DENETİMİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 – (1) Bu Yönetmeliğin amacı, Kurum gözetimi ve denetimi altındaki kuruluşların bilgi sistemleri ile iş süreçlerinin, bu Yönetmelik kapsamında yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ilgili usul ve esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Kurum gözetimi ve denetimi altındaki kuruluşlar ile bilgi sistemleri bağımsız denetimine ilişkin rapor oluşturulması amacıyla sınırlı olmak üzere bankaların konsolidasyon kapsamındaki ortaklıkları, bilgi sistemleri bağımsız denetimi yapmaya yetkili bağımsız denetim kuruluşları ve bilgi sistemleri bağımsız denetimi yapmak için dış hizmet alınan kuruluşlar 1 inci maddede belirtilen amaçla sınırlı olarak bu Yönetmelik hükümlerine tabidir.

Dayanak

MADDE 3 – (1) Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 15 inci, 36 ncı, 93 üncü ve 95 inci maddeleri, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanununun 14 üncü ve 17 nci maddeleri ile 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 27 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 – (1) Bu Yönetmelikte geçen;

a) Bağımsız denetçi: BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetçileri,

b) Bağımsız denetim: BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetimi,

c) Bağımsız denetim kuruluşu (BDK): BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetim kuruluşlarını,

ç) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,

d) BBDY: 2/4/2015 tarihli ve 29314 sayılı Resmî Gazete'de yayımlanan Bankaların Bağımsız Denetimi Hakkında Yönetmeliği,

e) BDY: Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunun 26/12/2012 tarihli ve 28509 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Yönetmeliğini,

f) Bilgi alışverişi kuruluşları: 5464 sayılı Kanunun 4 üncü maddesi çerçevesinde faaliyet izni alarak bilgi alışverişinde bulunan kuruluşları,

g) Bilgi sistemleri bağımsız denetimi: Bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ve denetlenenin faaliyetlerine ilişkin süreçler ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreci,

ğ) Bilgi sistemleri bağımsız denetim sicili (Sicil): Kurum tarafından elektronik ortamda tutulan ve bağımsız denetim kuruluşları ile denetçilerin kayıtlarının izlendiği sicili,

h) BSD: Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında bilgi sistemleri ve iş süreçleri bağımsız denetimi ile Kurum gözetimi ve denetimi altındaki diğer kuruluşlarda bilgi sistemleri bağımsız denetimini,

ı) Bilgi sistemleri denetimi dış hizmet kuruluşu (BSDDHK): BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz BDK'nın bu Yönetmelik kapsamında izin alarak BSD faaliyetini gerçekleştirmek için hizmet aldığı dış hizmet kuruluşunu,

i) Denetçi: Yetkili kuruluş ya da BSDDHK tarafından BSD yapmak üzere görevlendirilen ve unvanları 18 inci maddede sıralanan denetçi ile iş süreçleri denetimi faaliyetlerinde bulunan bağımsız denetçiyi,

j) Denetlenen: Kurum gözetimi ve denetimi altındaki kuruluşlar ile bu Yönetmelik kapsamında BSD raporu oluşturulması amacıyla sınırlı olmak üzere bankaların konsolidasyon kapsamındaki ortaklıklarını,

k) Dış hizmet: Bankalarda 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete'de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri dâhil olmak üzere; bu Yönetmelik kapsamındaki denetlenenlerin bilgi sistemlerine ilişkin dışarıdan temin ettikleri verilerin gizliliği, bütünlüğü ve erişilebilirliği ile sunulan hizmetlerinin sürekliliğini etkileme potansiyeli olan verilere erişimi bulunan ya da bu verilerin paylaşıldığı hizmet alımlarını,

l) Diğer finansal kuruluşlar: Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşları hariç Kurum gözetimi ve denetimi altındaki kuruluşları,

m) Genel kontroller: Bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli güven ortamının oluşturulmasını ve iş süreçleri üzerindeki kontrollerin işlevselliği için güvenilir bir ortamın sağlanmasını hedefleyen, bilgi sistemlerini oluşturan sistemler, bileşenler, süreçler ve verinin tamamına veya büyük bir bölümüne tatbik edilen kontroller ile bu kontrollerin tatbik edilmesini sağlayan politika ve prosedürleri,

n) İş süreçleri: Bankaların, Kanunun 4 üncü maddesi çerçevesinde yürüttüğü faaliyetlere ilişkin tesis edilen iş süreçleri ile Risk Merkezi ve bilgi alışverişi kuruluşlarının ilgili mevzuatı çerçevesinde yürüttükleri faaliyetler kapsamındaki iş süreçlerini,

o) Kanun: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununu,

ö) Kontrol: İş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

p) Kontrol hedefi: Belirli bir bilgi sistemleri aktivitesi içinde kontrol prosedürleri oluşturarak istenen bir sonucun veya bir amacın gerçekleştirilmesini sağlayan hedefleri,

r) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

s) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ş) Risk Merkezi: Kanunun ek 1 inci maddesi uyarınca Türkiye Bankalar Birliği nezdinde kurulan Risk Merkezini,

t) Yetkili kuruluş: Bu Yönetmelik kapsamında BSD yapma yetkisi verilen BDK'yı,

u) Yöneticiler: Denetlenenin yönetim kurulu, denetim komitesi ve kredi komitesi başkan ve üyeleri ile genel müdür, genel müdür yardımcıları ve imza yetkisine sahip mensuplarından; bölge müdürleri, şube müdürleri ve genel müdürlük merkez teşkilatında yer alan bölüm, kısım, grup ve bunlara eşdeğer isimler altında faaliyet gösteren birimlerin yöneticilerini,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Genel Kavramlar

Önemlilik

MADDE 5 – (1) Önemlilik; mesleki tecrübeye dayalı bir mütalaa konusu olup kontrol zayıflıkları sonucu ortaya çıkan ya da çıkabilecek hataların, ihmallerin, prosedürlere aykırılıkların ve hukuka aykırı fiillerin, denetlenenin finansal verilerini raporlamasına, güvenli ve kesintisiz hizmet sağlamasına olan ya da olabilecek etkisinin değerlendirilmesidir.

(2) BSD'de önemlilik kavramı, denetimin planlanması, gerekli alanlarda yoğunlaştırılması, bulguların değerlendirilmesi ve raporlanması için kullanılabilir.

(3) Denetlenen açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliği önemlilik kavramı kapsamında dikkate alınması gereken temel unsurlardır.

(4) Finansal raporları etkileyen kontrollerin değerlendirilmesinde, süreç veya sistem tarafından yürütülen finansal işlemin değeri, işlem sıklığı gibi öğeler kullanılırken, finansal işlemlere ilişkin olmayan kontrollerin değerlendirilmesinde ise iş sürecinin kritikliği, sistem ve operasyonların maliyeti, hataların muhtemel sonuçlarının büyüklüğü, bir zaman aralığında gerçekleşen işlem/sorgu sayısı, tutulan dosyaların ve üretilen raporların niteliği, zamanlaması ve kapsamı, hizmet seviyesi anlaşmalarının gerekleri ve ceza maddelerindeki para cezası tutarları gibi öğeler kullanılır.

Kontrol zafiyetlerinin sınıflandırılması

MADDE 6 – (1) Denetçi, incelemeleri neticesinde tespit ettiği kontrol zafiyetlerini önemlilik kavramına göre kontrol zayıflığı, kayda değer kontrol eksikliği ve önemli kontrol eksikliği şeklinde aşağıda belirtilen üç farklı sınıfta tasnif eder:

a) Kontrol zayıflığı: Bir kontrolün tasarımının veya işletilmesinin, hataları zamanında önleme ve tespit etmeye olanak sağlamaması durumudur.

1) Tasarımdaki kontrol eksikliği, bir kontrol hedefinin gerçekleşmesini sağlayacak kontrolün bulunmaması ya da var olan bir kontrolün tasarlandığı şekilde çalışıyor olsa bile tasarımındaki hatalardan dolayı kendisinden beklenen kontrol hedefini gerçekleştirememesi durumudur.

2) İşletimdeki kontrol eksikliği, düzgün tasarlanmış bir kontrolün tasarlandığı şekilde çalışmaması ya da kontrolü gerçekleştiren personelin, kontrolün etkin bir şekilde yerine getirilmesi için gerekli yetki ve yeterliliğe sahip olmaması durumudur.

b) Kayda değer kontrol eksikliği: Denetlenenin verilerinin bütünlüğünün, tutarlılığının, güvenilirliğinin ve gereken durumlarda gizliliğinin sağlanmasına, faaliyetlerinin devamlılığının teminine olumsuz etki yapması muhtemel bir kontrol zayıflığı veya birkaç kontrol zayıflığının bir araya gelmesi sonucu oluşan önemsiz sayılamayacak eksiklik olarak tanımlanır. İş süreçlerinde denetlenenin finansal verilerinin güvenilir bir şekilde genel kabul görmüş muhasebe

standartlarına uygun olarak kaydedilmesi, kayıtların yetkilendirilmesi, işlenmesi veya raporlanması sırasında oluşan hataların ve ihmallerin önlenmesine olumsuz etki yapması muhtemel eksiklikler de bu kapsamda değerlendirilir.

c) Önemli kontrol eksikliği: Bilgi sistemlerinin faaliyetlerini, verilerinin bütünlüğü, doğruluğu ile güvenliğini önemli düzeyde etkileyecek ve iş süreçlerinde denetlenenin dönemsel olarak yaptığı finansal raporlamalarında önemli bir yanlışlığın önlenmesini, düzeltilmesini engelleyecek veya bu süreçlere ilişkin bilgilerin bütünlüğünün ve tutarlılığının, güvenilirliğinin, devamlılığının ve gereken durumlarda gizliliğinin sağlanmasına önemli ve olumsuz etki etmesi kuvvetle muhtemel, bir veya birkaç kontrol zayıflığının bir araya gelmesidir.

Etkinlik, yeterlilik ve uyumluluk

MADDE 7 – (1) Bir kontrolün tasarımının etkin olarak kabul edilebilmesi için, tasarımdaki kontrol eksikliğinin bu kontrol bünyesinde bulunmaması veya bulunsa dahi önemli kontrol eksikliğine sebebiyet vermemesi gerekir.

(2) Bir kontrolün işletiminin etkin olarak kabul edilebilmesi için, işletimdeki kontrol eksikliğinin bu kontrol bünyesinde bulunmaması veya bulunsa dahi önemli kontrol eksikliğine sebebiyet vermemesi gerekir.

(3) Bilgi sistemleri ile iş süreçleri üzerindeki kontrollerin yeterli olması;

a) Önemlilik ilkesi çerçevesinde denetime tabi tutulan tüm kontrollerin tasarımlarının etkin olduğunu,

b) Bu kontrollerin; iş hedefleri çerçevesinde kendilerinden beklenen sonucu üretebilecek ve maruz kalınabilecek riskleri telafi edebilecek şekilde tasarlandıklarını,

ifade eder.

(4) Bilgi sistemleri ile iş süreçleri üzerindeki kontrollerin etkin olması;

a) Önemlilik ilkesi çerçevesinde denetime tabi tutulan tüm kontrollerin işletimlerinin etkin olduğunu,

b) Bu kontrollerin, kendilerinden beklenen işlevleri ve kontrol hedeflerini yerine getirdiklerini,

ifade eder.

(5) Bir kontrolün uyumlu sayılabilmesi için kontrole ilişkin kanunlar ve bu kanunlara istinaden yayımlanan alt düzenlemeler ve talimatlarda yer alan hususların ve yükümlülüklerin tamamının karşılanması gerekir. Önemlilik ilkesi çerçevesinde denetime tâbi tutulan tüm kontrollerin uyumlu olması, bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin uyumlu olduğunu ifade eder.

Denetim riski

MADDE 8 – (1) Denetim riski, denetçinin aşağıdaki risklere bağlı olarak doğru görüş vermemesi olasılığıdır:

a) Yapısal risk: Kontrolün olmaması nedeniyle, en azından kayda değer olan bir kontrol eksikliğinin var olması riskini ifade eder.

b) Kontrol riski: Kontrolün beklendiği gibi çalışmaması sebebiyle, en azından kayda değer olan bir kontrol eksikliğini önleyememesi, ortaya çıkaramaması veya zamanında düzeltememesi riskini ifade eder.

c) Tespit riski: Denetçinin, denetlenenin iç kontrol sisteminde yer alan en azından kayda değer olan bir kontrol eksikliğini ortaya çıkaramaması riskini ifade eder.

(2) Önemli veya kayda değer kontrol eksikliği riski: Denetlenenin iç kontrol sisteminde en azından kayda değer olan bir kontrol eksikliğinin bulunması riskini ifade eder. Önemli ya da kayda değer kontrol eksikliği riski, yapısal risk ve kontrol riskinden kaynaklanır.

(3) Denetçi, denetim riskini kabul edilebilir bir seviyeye indirmek için, önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde uygun denetim tekniklerini kullanır.

ÜÇÜNCÜ BÖLÜM
Yetkilendirme, İzin ve Denetçiler

Yetkilendirilecek kuruluşlarda aranan şartlar

MADDE 9 – (1) Bu Yönetmelik kapsamında bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında BSD yapmak için yetkilendirilecek kuruluşların;

a) BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz olması,

b) Bu Yönetmelik kapsamındaki faaliyetleri yürütecek yeterli sayı ve nitelikte denetçiye ve etkin bir bilgi sistemine sahip olması,

c) Kalite kontrol sistemine ilişkin yapı ve yazılı politikalar oluşturulması,

şarttır.

(2) Bu Yönetmelik kapsamındaki diğer finansal kuruluşlarda BSD yapmak için yetkilendirilecek kuruluşların;

a) Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından verilen kamu yararını ilgilendiren kuruluşlarda denetim yapma yetkisini haiz olması,

b) Bu Yönetmelik kapsamındaki faaliyetleri yürütecek yeterli sayı ve nitelikte denetçiye ve etkin bir bilgi sistemine sahip olması,

c) Kalite kontrol sistemine ilişkin yapı ve yazılı politikalar oluşturması,

şarttır.

Yetki başvurusu sırasında gerekli olan bilgi ve belgeler

MADDE 10 – (1) BSD faaliyetinde bulunmak isteyen BDK tarafından Kuruma verilecek başvuru dilekçesine, bilgi sistemleri bağımsız denetçilerinin;

a) Mesleki tecrübelerini, denetimle ilgili aldıkları eğitimleri, varsa katılmış olduğu denetim çalışmaları ve bu çalışmalarda almış olduğu görevleri de içeren Ek-1'de yer alan örneğe uygun olarak düzenlenecek ayrıntılı özgeçmişleri, lisans ve/veya lisansüstü eğitimlerine ilişkin diplomalarının/mezuniyet belgelerinin aslı ya da Kurumca onaylı sureti,

b) Varsa bilgi sistemleri ve bilgi teknolojilerine ilişkin alanlarda sahip oldukları sertifikaların aslı ya da Kurumca onaylı sureti,

c) Bu Yönetmelik kapsamına ilişkin konularda aldığı veya verdiği eğitimlere ilişkin belgelerin kopyaları,

ç) Adli sicil kaydı,

d) Bu Yönetmelik kapsamında uygun görülmüş olan unvanları,

e) Birden fazla BDK'da ortaklığının bulunmadığına dair Ek-2'de yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

f) Denetlenenlerde veya 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununa tabi şirketlerde denetim yapma yetkisi iptal edilmiş olan BDK'larda ortak veya yetki iptaline neden olan denetim faaliyetinde bağımsız denetçi veya denetçi sıfatı ile yer almadığına dair Ek-3'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

g) Mesleki faaliyetler dışında çalışmadıklarına dair Ek-4'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ğ) BDK'da tam zamanlı görev yaptıklarına veya yapacaklarına dair Ek-5'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

h) Daha önce yapılan ya da yapılacak bir disiplin kovuşturması sonucunda bağımsız denetimin yapılmasına engel teşkil edecek bir ceza alınmadığının ilgili kurumdan talep edilecek belge ile tevsik edilmesi kaydıyla, haklarında diğer yetkili kurumlar tarafından bir disiplin kovuşturması yapılıp yapılmadığına, böyle bir kovuşturma başlatıldığında en geç yedi gün içinde Kurumun bilgilendirileceğine, kovuşturma sonucunda BSD'nin yapılmasına engel teşkil edecek bir ceza alınması halinde bulunulan görevden en geç on beş gün içerisinde istifa edileceğine ilişkin, Ek-6'da yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ı) BSD faaliyeti sırasında bağımsızlıklarının ortadan kalkması durumunda denetlenene verilen bağımsız denetim hizmetinden çekileceğini taahhüt etmesine yönelik Ek-7'de yer alan örneğe uygun olarak düzenlenecek yazılı taahhüt belgesi,

eklenir.

(2) BDK'nın vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptıracaklarına ilişkin beyanlarına da başvuru dilekçesinde yer verilir.

BSD yapma yetkisinin verilmesi

MADDE 11 – (1) BSD yapma yetkisi almak üzere başvuruda bulunan BDK'lar bu Yönetmeliğin 10 uncu maddesinde belirtilen bilgi ve belgeler çerçevesinde Kurum tarafından değerlendirilir. Mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından yapılacak değerlendirme ve gerekirse yerinde incelemeler sonucunda faaliyet konularını yürütebilecek yeterliliğe sahip oldukları kanaatine varılması halinde BSD yapma yetkisi verilir, sicile kaydedilir ve bilgi sistemleri bağımsız denetim kuruluşları listesine eklenir.

(2) Yetki başvurularının değerlendirilmesi sürecinde, Kurum tarafından gerekli görülmesi halinde BDK'nın yetkinliğinin ve yeterliliğinin ölçülebilmesi amacıyla ilave bilgi ve belgeler talep edilebilir. Talep edilen bilgi ve belgeler yetkinin verilmesine ilişkin değerlendirmelerde dikkate alınır.

(3) Bu Yönetmelik kapsamında BSD yapma yetkisinin alınmasını sağlayan unsurların sürekliliği esastır. Kurum gerekli gördüğü durumlarda bu unsurların varlığını kontrol edebilir.

(4) Bu Yönetmelik kapsamında BSD yapma yetkisi verilen BDK'ların unvanları Kurum internet sitesinde duyurulur.

BSD yapma yetkisinin kaldırılması

MADDE 12 – (1) Aşağıdaki hallerin bir veya birkaçının tespit edilmesi halinde Kurul, yetkili kuruluşun BSD yapma yetkisini iki yıla kadar geçici olarak kaldırmaya yetkilidir:

a) Denetçiler tarafından kullanılan unvanların 18 inci maddede belirtilen hükümlere uygun olmaması.

b) Denetçilerin, denetlenenler ile Kuruma önceden bilgi verilmeden değiştirilmesi.

c) Bu Yönetmelik kapsamında Kurum tarafından uyarıyı gerektiren hususların üç denetim dönemi içerisinde tekrar edilmesi.

ç) Yeterli denetim kanıtı elde edilememesine rağmen olumlu görüş verilmesi.

d) Kurumca istenilen bilgi ve belgelerin verilmemesi.

(2) Aşağıdaki hallerin bir veya birkaçının tespit edilmesi halinde Kurul, yetkili kuruluşun BSD yapma yetkisini sürekli olarak kaldırmaya yetkilidir:

a) Denetime olan güveni sarsacak veya denetimi geçersiz kılacak derecede bağımsızlık ve tarafsızlık kaybedilerek BDY'nin 22 nci maddesine uygun hareket edilmeksizin BSD faaliyetinin gerçekleştirilmesi.

b) Birden fazla olmak üzere Kanunun 36 ncı maddesi uyarınca ve BBDY'nin 19 uncu maddesi kapsamında belirlenen usul ve esaslar çerçevesinde yaptırılması zorunlu olan mesleki sorumluluk sigortasının BSD'yi de kapsayacak şekilde yaptırılmaması.

c) Olumlu, şartlı ya da olumsuz görüş verilen BSD'nin, denetlenenin varlıklarının korunmasını, faaliyetlerin etkin ve verimli bir şekilde ilgili mevzuata, denetlenenin politika ve kurallarına uygun olarak yürütülmesini, muhasebe ve finansal raporlama sisteminin güvenilirliğini, bütünlüğünü, tutarlılığını ve bilgilerin zamanında elde edilebilirliğini sağlamasını önemlilik arz eden ölçüde etkileyecek hususlara yetkili kuruluş tarafından BSD raporunda yer verilmemiş olduğunun Kurumca tespit edilmesi halinde, yetkili kuruluşun bu hususta kusurlu olmadığını kanıtlayamaması.

ç) Birinci fıkra kapsamında yetkinin bir defadan fazla geçici olarak kaldırılması.

d) Bu Yönetmelik kapsamında devam eden BSD'ye ilişkin bir sözleşme bulunmaması ya da BSD'de, denetim sözleşmesinde yer alan unsurların gerçekleştirilmemesi veya eksik gerçekleştirilmesi.

e) 21 inci maddenin onuncu fıkrasına aykırılık oluşması.

f) Yetkili kuruluşun 9 uncu maddede belirtilen şartları kaybetmesi.

g) BSD raporunun yanıltıcı ve gerçeğe aykırı şekilde düzenlenmesi.

ğ) Kesintisiz olarak 5 yıl süreyle fiilen BSD faaliyetinde bulunulmamış olması.

(3) Birinci veya ikinci fıkra kapsamında tespit edilen hususların denetçiden kaynaklandığının veya BSD çalışmalarında yer alan denetçilerin dürüstlük, tarafsızlık, mesleki yeterlilik ve özen, bağımsızlık, güvenilirlik, mesleki davranış ve sır saklama gibi etik ilkelere uymadığının tespit edilmesi halinde Kurum, sorumluluğun içeriğine göre denetçilerin 18 inci maddede tanımlanan denetçi unvanlarını kullanarak BSD faaliyetlerinde bulunmasını geçici veya sürekli olarak yasaklayabilir.

(4) Yetkinin geçici veya sürekli olarak kaldırılmasından önce ilgili yetkili kuruluş ve/veya denetçinin savunması alınır. Savunma istendiğine ilişkin yazının tebliğ tarihinden itibaren bir ay içinde savunma verilmemesi halinde savunma hakkından feragat edildiği kabul edilir.

(5) Bu Yönetmelik kapsamında yetkili kuruluşun denetim yapma yetkisinin kaldırılması, bağımsız denetim yapma yetkisinin kaldırılması anlamına gelmez. Yetkili kuruluşun bağımsız denetim yapma veya bankalarda bağımsız denetim yapma yetkisinin kaldırılması halinde, bu Yönetmelik kapsamındaki denetim yapma yetkisi hiçbir işleme gerek kalmaksızın kaldırılmış sayılır.

(6) BSD yapma yetkisi geçici olarak kaldırılan yetkili kuruluş söz konusu süre sonunda yasağın kaldırılması için Kuruma başvurur; başvuru yapılmadığı takdirde yasak uygulanmaya devam eder. Kuruma yapacakları başvurular, yetkili kuruluş hakkında devam etmekte olan bir inceleme olup olmadığı da dikkate alınarak Kurulca değerlendirilerek karara bağlanır.

(7) BSD yapma yetkisi geçici olarak kaldırılan denetçi, söz konusu süre sonunda yasağın kaldırılması için Kuruma başvurur; başvuru yapılmadığı takdirde yasak uygulanmaya devam eder. Kuruma yapacakları başvurular, denetçi hakkında devam etmekte olan bir inceleme olup olmadığı da dikkate alınarak Kurumca değerlendirilerek karara bağlanır.

(8) Bu Yönetmelik kapsamında BSD yapma yetkisi kaldırılan BDK'ların unvanları Kurum internet sitesinde duyurulur.

BSD'nin dış hizmet alımı ile gerçekleştirilmesi

MADDE 13 – (1) BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz BDK Kurumdan izin alarak BSD faaliyetini dış hizmet alımı yoluyla gerçekleştirebilir.

(2) BDK'nın, BSD'yi dış hizmet alımı yoluyla gerçekleştirmesi durumunda da, ilgili faaliyetler ve bu Yönetmelik kapsamındaki yükümlülüklerden kendisi ve BSDDHK adına nihai anlamda sorumludur.

(3) Aynı BSDDHK birden fazla BDK'ya hizmet verebilir.

(4) Bir BDK bir seferde en fazla üç dönem için dış hizmet alımı ile BSD yapma izni başvurusunda bulunabilir. İzin süresi dolduğunda ilgili BDK dış hizmet alımı ile BSD yapma izni için tekrar başvuruda bulunabilir.

(5) Kurum, BSDDHK'lardan denetlenenin tabi olduğu kanun ve bu Yönetmelik hükümleri ile ilgili göreceği bütün bilgileri gizli dahi olsa istemeye, tüm kayıt ve belgelerini incelemeye yetkili olup, BSDDHK'da istenilen bilgileri vermekle yükümlüdür.

BSDDHK'da aranan şartlar

MADDE 14 – (1) BDK'nın BSD faaliyetini gerçekleştirmek üzere hizmet alacağı BSDDHK'ların;

a) Denetçilerinin bu Yönetmelikte tanımlanan denetçi niteliklerini haiz olması,

b) Denetim ekipleri içerisinde yeterli sayıda ve nitelikte denetçi istihdam etmesi,

c) Denetçisinin, geçmişte görev aldığı BSD faaliyetlerinde, denetim ilkelerine bağlı ve denetçi bağımsızlığı ilkesini zedelememiş olması,

ç) BDY'nin 26 ncı maddesinin birinci fıkrasının (ç) bendinde belirtilen koşulları sağlaması,

şarttır.

(2) BSDDHK'nın BSD gerçekleştirebilmesi için bu Yönetmelik kapsamında, BDK ile sözleşme yapmış olması gereklidir. Bu sözleşme ile BDK, BSDDHK'nın denetim ilkelerine bağlılığını; bu Yönetmelik ve ilgili diğer düzenlemeler kapsamındaki hususlara ilişkin hükümlere uymasını sağlamak zorundadır.

İzin başvurusu sırasında gerekli olan bilgi ve belgeler

MADDE 15 – (1) BSD faaliyetinde dış hizmet alımında bulunmak isteyen BDK, Kuruma vereceği başvuru dilekçesine;

a) BDK ve BSDDHK ile ortakları ve denetçilerine ilişkin 10 uncu maddenin birinci ve ikinci fıkraları kapsamında yer verilmesi gereken belgeleri,

b) BDK ile BSDDHK arasında yapılmış olan, tarafların sorumluluklarının, denetim planının açıkça belirtildiği, BSDDHK'nın BSD raporunu imzalamakla yetkilendirdiği Bilgi Sistemleri Bağımsız Başdenetçisi, denetim ilkeleri, denetçi bağımsızlığı, gizlilik ve çıkar çatışması, denetim ekipleri ve saatlik denetim ücreti ile toplam hizmet bedeli gibi hususların açıklığa kavuşturulmuş olduğu sözleşmeleri,

c) BSDDHK'nın merkezinin varsa şube ve/veya şubelerinin adreslerini,

ç) BSDDHK'nın başvuru tarihindeki bilançosunu,

d) BSDDHK'nın yurt dışında yerleşik bir şirket ile dış hizmet alımına konu alana ilişkin hukuki bağlantısı olması durumunda, ilgili şirket ile yapılan sözleşmelerin şirket yetkililerince tasdik edilmiş kopyasını,

e) BSDDHK'nın denetçilerinin, denetim ilkelerine bağlı olmak, gizlilik ve denetçi bağımsızlığı ilkesini zedelememek koşuluyla BSD'de görev alacaklarına dair Ek-8'de yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ekler.

Dış hizmet alımı ile bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimi yapma izninin verilmesi

MADDE 16 – (1) Dış hizmet alımı ile BSD yapma iznini almak üzere başvuruda bulunan BDK ile BSDDHK'nın bilgi ve belgeler çerçevesinde değerlendirilerek, mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından gerektiğinde yerinde incelemede bulunulması neticesinde, faaliyet konularını yürütebilecek yeterliliğe sahip oldukları kanaatine varılması halinde, Kurul kararıyla, uygun görülen dönemler için BSD yapma izni verilir.

(2) BDK'nın dış hizmet alacağı kuruluşun bu Yönetmelik kapsamında yetkili bir kuruluş olması durumunda dış hizmet alımı ile BSD yapması Kurum değerlendirmesine tabidir.

(3) Dış hizmet alımı ile BSD yapma izni alan BDK ve BSD çerçevesinde sunduğu hizmetle sınırlı olmak üzere ilgili BSDDHK bu Yönetmelik kapsamında, aksi belirtilmedikçe, yetkili kuruluşlarla ilgili bütün hükümlere tâbidir.

Dış hizmet alımı ile bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimi yapma izninin iptali

MADDE 17 – (1) Bu Yönetmelik hükümlerine aykırı hareket ettikleri tespit edilen dış hizmet alımı ile denetim yapma izni alan BDK'lar ve ilgili BSDDHK'larda 12 nci maddenin birinci ve ikinci fıkralarında yer verilen hususların bir veya birkaçının varlığının tespiti halinde, aykırılıkların mahiyetine bağlı olarak, Kurum tarafından yapılan değerlendirme üzerine Kurul, BDK'nın dış hizmet alımı ile BSD yapma iznini geçici veya sürekli olarak kaldırır.

(2) Kurumun birinci fıkra kapsamında dış hizmet alımı ile BSD yapma yetkisini geçici ya da sürekli kaldırması durumunda, BSDDHK'nın ilgili denetçilerinin yetki kaldırılmasına sebep olan hususlarda sorumluluğunun içeriğine göre 18 inci maddede tanımlanan denetçi unvanlarıyla BSD faaliyetlerinde bulunmasını Kurum geçici veya sürekli olarak yasaklayabilir.

(3) BDK ve BSDDHK arasındaki sözleşmenin feshedilmesi halinde yedi gün içinde Kuruma bilgi verilir.

Denetçi unvanları

MADDE 18 – (1) Bu Yönetmelik kapsamında denetçiler kıdem sırasına göre Bilgi Sistemleri Bağımsız Başdenetçisi, Bilgi Sistemleri Bağımsız Kıdemli Denetçisi, Bilgi Sistemleri Bağımsız Denetçisi unvanlarını alırlar. Bu unvanlar haricindeki oluşturulacak unvanlar ve bu unvanların taşıması gereken şartları BDK takdirindedir.

(2) Bilgi sistemleri denetimi, bilgi sistemleri kontrolü veya güvenliği, yazılım geliştirme ve bilgi teknolojileriyle ilgili konularda fiilen geçirilen çalışma sürelerinin toplamı bu Yönetmelik kapsamında mesleki tecrübe olarak kabul edilir.

(3) Bilgi Sistemleri Bağımsız Denetçisinin aşağıdaki şartları taşıması zorunludur:

a) Üniversitelerin veya denkliği yetkili makamlarca kabul edilen yurt dışındaki yükseköğretim kurumlarının 4 yıllık lisans programlarını tamamlamış olmak.

b) En az 1 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 3 yıl mesleki tecrübeye sahip olmak.

(4) Bilgi Sistemleri Bağımsız Kıdemli Denetçisinin aşağıdaki şartları taşıması zorunludur:

a) Bilgi Sistemleri Bağımsız Denetçisi unvanını haiz olabilmek için aranan şartlara sahip olmak.

b) En az 2 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 6 yıl mesleki tecrübeye sahip olmak.

(5) Bilgi Sistemleri Bağımsız Başdenetçisinin aşağıdaki şartları taşıması zorunludur:

a) Bilgi Sistemleri Bağımsız Denetçisi unvanına sahip olabilmek için aranan şartları haiz olmak.

b) En az 3 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 10 yıl mesleki tecrübeye sahip olmak.

(6) Beşinci fıkradaki şartları taşıyan denetçiler Kurumca yapılan değerlendirmeler sonucunda uygun görülmesi halinde Bilgi Sistemleri Bağımsız Başdenetçisi unvanına sahip olurlar ve sicile kaydedilirler. Kurum, Bilgi Sistemleri Bağımsız Başdenetçisi unvanını denetimin yapılacağı kuruluşa göre şartlı verebilir.

(7) Bilgi Sistemleri Bağımsız Başdenetçisi unvanı haricindeki diğer denetçi unvanlarına yapılan terfiler yetkili kuruluşlar tarafından yapılır, Kurumca belirlenen usul ve esaslara uygun olarak Kuruma bildirilir. Bilgi, yetenek ve

liyakatleri bir üst kıdemin gerektirdiği nitelikte olmayanlar tecrübe şartını sağlasalar dahi bir üst unvana terfi ettirilemezler.

(8) Bu Yönetmelik kapsamındaki yetkili kuruluşların BSD'yle görevlendirilmiş denetçilerinin tümünün, yılda en az yirmi saat, üç yılda en az yüz yirmi saat BSD kapsamında sürekli eğitim almaları veya vermeleri zorunludur.

(9) Kurumun BSD yapmakla görevli daire başkanlığında bu madde kapsamında belirtilen sürelerde görev yapmış meslek personeli ilgili unvanı haiz kabul edilir. Bu kapsamda 10 yıllık mesleki tecrübeye sahip meslek personeli de Bilgi Sistemleri Bağımsız Başdenetçisi unvanını alır ve sicile kaydedilir.

DÖRDÜNCÜ BÖLÜM
Tarafların Yükümlülükleri

Denetlenenin yükümlülükleri

MADDE 19 – (1) Denetlenen, bilgi sistemleri dokümantasyonunu, iş süreçlerine ait dokümantasyonu ve bu dokümantasyonla ilgili her türlü kayıt, bilgi, belge, yapı ve sistemlerini BSD'ye uygun ve hazır hale getirmek zorundadır.

(2) Denetlenen, denetçinin BSD'ye yönelik talep ettiği gizli dahi olsa her türlü bilgi ve belgeyi vermekle yükümlüdür.

(3) Denetlenen, denetçilere faaliyetlerinde kullandıkları tüm sistem ve uygulamaları kullanım amaçlarını kapsayan uygulama listesiyle birlikte bildirmek; kontrol mekanizmalarına ilişkin dokümantasyonu ve uygulamalarına ilişkin kullanıcı dokümanlarını, bankalar ayrıca 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 9 uncu maddesi uyarınca hazırladığı iş akım şemalarını da sunmakla yükümlüdür.

(4) Denetlenen, denetçi tarafından BSD kapsamında talep edilen iç denetim ve iç kontrol raporlarının bir örneğini denetçiye iletir ve 35 inci madde kapsamında denetçi ile personeli arasındaki iş birliğinin sağlanması için gerekli tedbirleri alır, yetkili kuruluşun denetçileri tarafından yöneltilen soruların zamanında yanıtlanmasını ve ilgili konulara açıklık getirilmesini sağlar.

(5) Denetçilerce yapılacak tespitler hakkında denetlenenin yönetim kurulunun bilgilendirilmesi; bağımsız denetçiler ile yönetim kurulu üyeleri ve denetlenen personeli arasında koordinasyonun sağlanması bankalarda banka denetim komitesinin, Risk Merkezinde Risk Merkezi yönetiminin ve diğer denetlenenlerde ise yönetim kurulunun sorumluluğundadır.

(6) Denetlenen tarafından sözleşme süresi içinde anlaşmalı olunan yetkili kuruluşun değiştirilmesi istendiği ya da yetkili kuruluş tarafından BSD sözleşmesine aykırı hareket edildiği ve/veya BSD'nin bu Yönetmelikte belirtilen esaslara göre yapılmadığı hallerde, durumun gerekçesiyle birlikte Kuruma bildirilmesi ve BSD sözleşmesinin feshedilebilmesi için Kurumun uygun görüşünün alınması zorunludur.

(7) Denetlenen, BSD raporunda ortaya konulan bulguların çözümlerine ilişkin taahhütlerini bir aksiyon planı ile karara bağlar. Aksiyon planının yürütülmesinin ve bu planda yer alan taahhütlerin zamanında ve eksiksiz olarak yerine getirilmesinin sağlanmasından denetlenen yönetim kurulu sorumludur. Aksiyon planının hazırlanması ve raporlanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Yönetim Beyanı

MADDE 20 – (1) Banka, yönetim kurulu tarafından denetim dönemi itibarıyla düzenlenen Yönetim Beyanını denetçiye sunar. Yönetim Beyanı ile yönetim kurulu, 15/3/2020 tarihli ve 31069 sayılı Resmî Gazete'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin 32 nci maddesi kapsamında yapılan çalışmalara ve bankacılık süreçlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, mevcut durum ve yürütülen çalışmalara ilişkin güvence sunar.

(2) Yönetim Beyanına mesnet teşkil edecek çalışmalar, banka iç sistemler birimlerince bu Yönetmeliğin beşinci ve altıncı bölümleri çerçevesindeki usul ve esaslar dikkate alınarak gerçekleştirilir.

(3) Banka Yönetim Kurulu, Yönetim Beyanını, cari BSD dönemine ilişkin yürütülen çalışmalar ve değerlendirmeler neticesinde oluşturur. Bu bağlamda esas alınacak dönem 1 Ocak-31 Aralık dönemi olup, Banka Yönetim Kurulu bu dönemin sonu itibarıyla, BSD raporu tarihi ile uyumlu olarak beyanda bulunur.

(4) Yönetim Beyanında asgari olarak;

a) Banka Yönetim Kurulunun 5411 sayılı Kanunun 29 uncu ve 30 uncu maddeleri ve Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 4 üncü maddesinin birinci fıkrasına istinaden etkin, yeterli ve uyumlu bir iç kontrol sistemi kurma ve işletme yükümlülüğünün bulunduğu,

b) İlgili banka birimlerince, iç kontrol sisteminin incelenmiş ve bu sistem hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılmış olduğu,

c) İç kontrol sistemi üzerinde -varsa- tespit edilen önemli kontrol eksiklikleri,

ç) İç kontrol sistemi üzerinde yapılan değerlendirmelerde -dönem sonu itibarıyla düzeltilmiş olsa dahi- tespit edilen iç kontrol sistemine ilişkin tüm kontrol zayıflıklarının, kayda değer ve önemli kontrol eksikliklerinin sınıflandırılarak denetçiye sunulduğu,

d) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere banka açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen ya da önemli seviyede olmasa da yöneticilerin veya iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu tüm suistimal veya yolsuzluklar,

e) İç kontrol sisteminde gerçekleştirilen incelemeleri takiben, önemli ve kayda değer kontrol eksiklikleri konularında banka tarafından alınmış olan düzeltici önlemleri de içerecek şekilde, iç kontrol sisteminde veya iç kontrol sistemini önemli derecede etkileyebilecek diğer hususlarda meydana gelmiş olan değişiklikler,

beyan edilir.

(5) Yönetim Beyanı kapsamında;

a) Bankacılık süreçleri iç denetimlerinin kritik banka servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olması,

b) Bankacılık süreçleri iç denetimlerinin sıklığı ve denetim döngülerinin; banka servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olması,

c) 25 inci maddede yer alan süreçlere ilişkin kontrollere güvence vermek üzere yapılacak bankacılık süreçleri iç denetimleri için denetim döngüsünün her yıl olması,

ç) Yapılan denetimlere ilişkin çalışma kanıtlarının en az üç yıl banka nezdinde saklanması,

esastır.

(6) Yönetim Beyanı, denetim dönemini takip eden Ocak ayı sonuna kadar bağımsız denetim kuruluşuna iletilir.

(7) BDK, Yönetim Beyanını ve bu beyana mesnet teşkil eden çalışmaların yeterliliğini inceler. Denetçi beyanda, içerik açısından eksiklik veya bağımsız denetim çalışması sonuçları itibarıyla varsa uyumsuzlukları tespit eder. BDK Yönetim Beyanına ilişkin değerlendirme ve tespitlerine BSD'de ayrı bir bölüm halinde yer verir.

Yetkili kuruluşların ve denetçilerin yükümlülükleri

MADDE 21 – (1) Denetçiler bu Yönetmelik ile BDY'nin 21 inci maddesinin birinci fıkrasında belirlenen ilkelere uymak, bilgi sistemleri ve iş süreçleri içerisinde yer alabilecek riskleri ve zayıflıkları dikkate alarak ve mesleki şüphecilik çerçevesinde bir denetim planı hazırlamak, denetlenene sunmak ve uygulamak, yöneticilerin açıklamalarını yeterli denetim kanıtı olarak kabul etmemek ve BSD raporunu oluşturmak ile yükümlüdür.

(2) BDY'nin 20 nci maddesine göre BDK tarafından tesis edilmesi gerekli olan kalite kontrol sistemi bu Yönetmelik kapsamında yapılan BSD çalışmalarını ve BSD raporlarını da kapsayacak şekilde yürütülür.

(3) Denetçi, ortaya çıkan hata ve suistimaller hakkında denetlenenin yöneticilerine ve denetlenenin iç sistemlerden sorumlu yönetim kurulu üyelerine her aşamada yazılı olarak bilgi vermek zorundadır.

(4) 10 uncu maddede belirtilen belge ve beyanlardaki değişikliklerin yedi gün içerisinde Kuruma bildirilmesi zorunludur. Denetim kadrosunda meydana gelen değişiklikler, gerekçeleri ile birlikte Kurumca belirlenen usul ve esaslara uygun olarak Kuruma bildirilir.

(5) Yetkili kuruluş, sözleşme süresi içinde BSD'den çekilmesi ya da sözleşmenin feshedilmesi hallerinde, durumu gerekçesiyle birlikte yedi gün içerisinde Kuruma bildirmek zorundadır.

(6) BSD faaliyeti sırasında, esas alınan mevzuat hükümlerine uymayan işlemlerin veya olumsuz görüş oluşturmaya veya görüş bildirmekten kaçınmaya yol açabilecek herhangi bir gelişmenin tespit edilmesi durumunda, denetlenen bunları gidermiş olsa dahi, denetçi bu hususu on beş gün içinde Kuruma yazılı olarak bildirir. Kanuna ve diğer kanunlara göre konusu suç teşkil eden hallerde durumun ivedi olarak yetkili mercilere intikali sağlanır ve ayrıca Kuruma yazılı olarak bilgi verilir.

(7) Denetçi, aşağıda belirtilen konular da dâhil olmak üzere BSD sırasında ortaya çıkan ve önemli bulduğu her konuda ilgili yöneticileri yazılı veya sözlü olarak derhal bilgilendirir:

a) Muhtemel kısıtlamalar ve ilave çalışmalar da dâhil olmak üzere BSD'nin genel yaklaşımı ve kapsamı.

b) Bilgi sistemleri ve iş süreçleri üzerinde önemli bir etkisi olan ya da olabilecek politika oluşturma süreci ile ilgili aksaklıklar, politika uygulamalarındaki sorunlar ya da politika uygulamalarındaki değişiklikler.

c) Denetlenenin faaliyetlerinin sürekliliği üzerinde şüphe uyandırabilecek belirsizlikler.

ç) Bilgi sistemlerine ve iş süreçlerine veya BSD raporuna önemli etkisi olabilecek konularda yöneticilerle olan görüş aykırılıkları.

d) Bilgi sistemleri ve iş süreçleri içerisinde yer alan önemli zayıflıklar ve riskler.

(8) Sözlü olarak bilgilendirmenin yapıldığı durumlarda denetçi çalışma kâğıtlarında bildirilen hususları ve alınan cevapları belgelendirir.

(9) Denetçiler, BSD çerçevesinde ilgililerce kendilerine tevdi edilen dokümantasyon ve belgeleri işlerinin gerektirdiği süre içinde iyi niyetle, güvenli şekilde ve değiştirmeden muhafaza etmekle ve işin bitiminde iadesiyle yükümlüdürler. Denetim kanıtı oluşturan dokümanların kopyaları yetkili kuruluş tarafından saklanabilir.

(10) Yetkili kuruluşlar ve denetçiler, BSD faaliyetleri dolayısıyla öğrendikleri ve ilgili düzenleme hükümlerine göre sır kapsamında bulunan bilgilerin kendi nezdinde korunmasına ilişkin tedbirleri alır, bu bilgileri kanunen açıkça yetkili kılınanlardan başkasına açıklayamaz ve doğrudan veya dolaylı şekilde kendi yararlarına kullanamazlar. Bu

yükümlülük görevden ayrıldıktan sonra da devam eder. Bu çerçevede asgari olarak aşağıda yer verilen hususlar dikkate alınır:

a) Yetkili kuruluşlar BSD sırasında elde ettikleri kendi nezdinde bulunan sır kapsamındaki verilerin ve BSD kapsamında kullandıkları sistemlerin güvenliğine ilişkin politika, prosedür ve süreçleri tesis ederler.

b) Yetkili kuruluşlar bünyelerinde bulunan sır kapsamındaki verilerin yer aldığı veri tabanlarına, BSD sürecinde kullanılan uygulamalara ve sistemlere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Görev ve sorumluluklar göz önünde bulundurularak, gerekli olan en kısıtlı yetki ve erişim hakkı verilir. Yetkiler ve erişim hakları en az yetki prensibi açısından asgari yılda bir kez gözden geçirilir.

c) BSD kapsamında yetkili kuruluşa ait bilgi sistemleri üzerinde gerçekleşen işlemler için işlemlerin türü, niteliği ve verinin hassasiyet derecesi dikkate alınarak uygun bir kimlik doğrulama mekanizması kurulur. Aynı kullanıcı hesabının birden fazla kişi tarafından kullanılması engellenir ve kimlik doğrulamada inkâr edilmezlik sağlanır.

ç) Yetkili kuruluşun BSD faaliyetlerine ilişkin bilgi sistemleri üzerinde etkin bir denetim izi mekanizması tesis edilir. Bilgilere erişilmesi, sorgulanması, bunlara yönelik erişim yetkilerinin verilmesi veya değiştirilmesine yönelik işlemler ve bunlara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları tutulur.

(11) Denetlenen tarafından BSD'ye ilişkin bilgi ve belgelerin yetkili kuruluşa verilmemesi halinde bu durum Kuruma ivedilikle bildirilir.

(12) Yetkili kuruluşların denetçilerinde yapılan değişikliklerin Kurumca belirlenen usul ve esaslara uygun olarak Kuruma bildirilmesi zorunludur. Kurumca yapılan değerlendirme neticesinde kırk beş gün içerisinde olumsuz görüş bildirilmeyen değişiklikler geçerli sayılır.

(13) Yetkili kuruluş, BSD'den kaynaklanabilecek riskleri karşılayabilecek kapsamda mesleki sorumluluk sigortası yaptırmakla yükümlüdür.

(14) Yetkili kuruluş, istihdam ettiği denetçiler tarafından bu Yönetmelik kapsamında düzenlenecek çalışma kâğıtlarını ve BSD'ye ilişkin her türlü bilgi, belge ve sistemi istenildiğinde Kuruma göndermek ya da Kurumun denetime yetkili meslek personeline sunmak zorundadır.

(15) Yetkili kuruluşlar ve denetçileri BSD sözleşmesi öncesinde BDY'nin 26 ncı maddesinin birinci fıkrasının (ç) bendinde belirtilen koşulları sağlamakla yükümlüdür.

(16) Yetkili kuruluşlar ve denetçileri bu Yönetmelikte düzenleme bulunmayan konularda Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından yayımlanan Bağımsız Denetçiler İçin Etik Kurallar Standardı (Bağımsızlık Standartları Dâhil)'na uyarlar.

(17) Yetkili kuruluşlar bilgi sistemleri ve iş süreçleri konularında danışmanlık hizmeti verdikleri şirketleri farklı bir yetkili kuruluş tarafından denetlenmediği müddetçe denetleyemezler.

(18) Bu Yönetmelik kapsamında yetkilendirilen kuruluşlar, birincil sistemlerini ve her türlü yedeğini yurt içinde bulundurmak zorundadır. Yetkilendirilen kuruluşların faaliyetlerini yürütürken kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için sistem veya uygulama üzerinden herhangi bir denetim sürecinin yürütülmemesi, denetlenene ait verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir.

BEŞİNCİ BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Esaslar

BSD'nin kapsamı

MADDE 22 – (1) Bu Yönetmelik kapsamında yapılacak olan denetim çalışması, 24 üncü maddede tanımlanan bilgi sistemleri bağımsız denetimi ile 25 inci maddede tanımlanan iş süreçleri bağımsız denetiminden oluşur.

(2) Denetçi, denetlenenin bilgi sistemleri ve iş süreçleri kapsamında inceleyeceği süreç, sistem, faaliyet ve kontrol mekanizmalarını, risk odaklı bir bakış açısıyla ve önemlilik kriterini esas alarak yazılı olarak belirler. Bununla birlikte denetçi, önemlilik kriteri çerçevesinde belirlediği denetimlerin kapsamının; bu Yönetmelik kapsamında oluşturacağı denetim görüşüne makul güvence sağlamak için yeterli denetim kanıtı elde edecek şekilde olmasını temin eder.

(3) Denetlenenin iç kontrol sistemiyle ilgili olarak iç sistemleri bünyesinde yürütülen faaliyetler, 26 ncı madde kapsamında ve iş süreçleri bağımsız denetimi dâhilinde incelenir.

(4) Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında iş süreçleri bağımsız denetimi her yıl, bilgi sistemleri bağımsız denetimi ise iki yılda bir kez yapılır. BSD yapılmayan yıllarda denetçi geçmiş dönemden gelen bulguları değerlendirir ve ayrıca bilgi sistemi ortamında meydana gelen önemli değişiklikler ve önemlilik kriteri kapsamında incelenmesini gerekli gördüğü süreçleri denetim kapsamına alabilir. Süreçlerin kapsama alınma sebeplerine ilişkin değerlendirmelere raporda yer verilir.

(5) Diğer finansal kuruluşlarda bilgi sistemleri bağımsız denetimi üç yılda bir yapılır.

(6) Kurum, gerekli gördüğü hallerde denetlenenlerden herhangi biri ya da tüm denetlenenler için, bu denetimlerin kapsamını ve sıklığını farklılaştırabilir.

(7) Bankalar için konsolide BSD kapsamında bağımsız denetime tâbi tutulacak kuruluşlar, denetlenenin konsolide finansal tablolarının oluşturulmasına ilişkin Kurum tarafından yapılan düzenlemelerde yer alan ve konsolide

finansal tabloların oluşturulmasına dahil edilecek kredi kuruluşu veya finansal kuruluş niteliğine sahip kuruluşların tespitinde esas alınan hükümler doğrultusunda belirlenir.

(8) Denetçi, yedinci fıkra uyarınca bağımsız denetime tâbi tutacağı ortaklıklarda gerçekleştireceği BSD kapsamını, önemlilik kriterini kullanarak, konsolidasyona esas finansal bilgiyi üreten bilgi sistemleri ve süreçler üzerindeki kontrollerin etkinlik, yeterlilik ve uyumluluğunun tespit edilmesini sağlayacak şekilde yazılı olarak belirler.

(9) Yetkili kuruluşlar denetimden sorumlu bir Bilgi Sistemleri Bağımsız Başdenetçisi atarlar ve denetimin kapsamına uygun ve yeterli sayıda denetçiden oluşan bir denetim ekibi oluşturulmasını sağlarlar.

Bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimi ile bağımsız denetimin ilişkisi

MADDE 23 – (1) Bağımsız denetim ile BSD; birbirlerinin kapsam ve sonucunu etkileyecek hususlar ihtiva etmeleri nedeni ile bütünsel bir yaklaşım içinde planlanır ve uygulanır.

(2) Yetkili kuruluşların, Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında BSD gerçekleştirileceği dönemde, denetlenenin bağımsız denetim faaliyetini de yürütüyor olmaları zorunludur.

(3) Denetçi BSD kapsamını belirlerken ve bu kapsamdaki çalışmalarını yürütürken; denetim görüşünü destekleyecek düzeyde yeterli ve uygun denetim kanıtı elde edilmesinin yanı sıra, bağımsız denetime ilişkin denetim riski değerlendirmelerini desteklemek için de denetim kanıtı elde edilmesini gözetir.

(4) Bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimine ilişkin görüşün şartlı, olumsuz ya da görüş bildirmekten kaçınma şeklinde olması durumunda; görüş ve görüşe esas teşkil eden tespitler bağımsız denetçiye yazılı olarak iletilir.

(5) Yetkili kuruluş, Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında gerçekleştireceği bilgi sistemleri ve iş süreçleri denetimi döneminde, denetlenenin bağımsız denetim faaliyetini de eşgüdümlü olarak yürütür.

Bilgi sistemleri bağımsız denetimi

MADDE 24 – (1) Denetçi, bilgi sistemleri genel kontrollerini, önemlilik kriterini esas alarak belirlediği kapsam dâhilinde etkinlik, yeterlilik ve uyumluluk açısından incelemeye tâbi tutar.

(2) Genel kontroller, tesis edilmelerinde esas alınan çerçeve, standart ya da metodolojiden bağımsız olarak; denetlenenin bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin Kurum tarafından yapılan düzenlemelerdeki hükümler gözetilerek denetlenir.

İş süreçleri bağımsız denetimi

MADDE 25 – (1) Denetçi, denetlenenin tabi olduğu mevzuat çerçevesinde yürüttüğü faaliyetlere ilişkin iş süreçlerini ve bu süreçler üzerindeki iç kontrollerini, önemlilik kriterini esas alarak belirlediği kapsam dâhilinde etkinlik, yeterlilik ve uyumluluk açısından incelemeye tâbi tutar.

(2) Bankalarda iş süreçlerinin bağımsız denetimi kapsamında bankacılık faaliyetlerine ilişkin aşağıda yer alan süreçler ve gerekli görülen diğer süreçler ile ilgili hususlar önemlilik kriteri çerçevesinde dikkate alınarak değerlendirilir:

a) Mevduat süreci: Mevduat/katılma hesaplarına ilişkin işlemler, çek/senet, fon transferi ve tahsilat işlemleri, mevduatın sınıflandırılması, tasarruf mevduatı kapsamının belirlenmesi ve tasarruf mevduatı sigorta primlerinin hesaplanması gibi hesaplama kontrolleri, katılma hesaplarına ödenecek kar payı tutarlarının günlük birim değer hesap tablosu üzerinden hesaplanmasına ilişkin kontroller, şüpheli işlem tespiti ve suç gelirlerinin aklanması ve terörün finansmanına ilişkin kontroller, işlemlerin muhasebeleştirilmesi ve süreçteki diğer kontroller.

b) Bireysel/Kurumsal kredi süreçleri: Kredi başvurularının alınması, değerlendirilmesi, kredi tahsisi, kullandırım işlemleri ve onayları, teminatlandırma, kredi limitleri ile kredi geri ödeme tabloları ve hesaplamalarına ilişkin kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, kredilerin sınıflandırılması, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, kredi risklerinin ölçülmesi, izlenmesi, kontrolünün sağlanması, raporlanması ve riskleri karşılayacak yeterli sermayenin ayrılması, kredilere getirilen vade, faiz/kar payı, komisyon ve benzeri sınırlarının takibi, kredi işlemlerinin muhasebeleştirilmesi ve diğer süreç kontrolleri.

c) Muhasebe süreci: Faiz, gelir/gider tahakkuku ve reeskont hesaplamaları, işlem bazında tek düzen hesap planına uygunluk, amortisman hesaplamaları, muhasebe fişi kesilmesine ilişkin yetkilendirme süreci, mizanın oluşumu, geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı ve ilgili kayıtların bütünlüğü ve izlenebilirliği, işlem numaralarının ardışıklığının sağlanması, işlem limitlerinin ve yetkilerinin kontrolü, şube ve genel müdürlük kayıtları arasındaki mutabakatlar, hesap planı düzenleme ve değişikliklerine ilişkin kontroller, defteri kebir hesapları ile yardımcı, alt ve geçici hesapların mutabakatı, yasal ve yardımcı defterler arası mutabakatlar, muhasebe kayıtlarının arada başka bir muhasebe sistemini referans almaksızın tek düzen hesap planına ve Türkiye Muhasebe Standartlarına uygun olarak doğrudan oluşturulması, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri.

ç) Banka ve kredi kartları süreci: Banka ve kredi kartı başvuru değerlendirme, limit tahsisi, kart basım ve dağıtım işlemleri, kart iptali, üye işyeri ve üye işyeri anlaşma yapan kuruluşların yükümlülüklerinin kontrolleri, kart ve POS teknik altyapısına ilişkin kontroller, kartların kullanımı ve hediye puanı gibi uygulamalara ilişkin kontroller, kayıp/çalıntı kartlara ilişkin kontroller, şüpheli işlemlerin takibi ve tespiti, sahtecilik ve dolandırıcılık olaylarının önlenmesine yönelik kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, banka ile kart merkezi mutabakatları gibi mutabakat kontrolleri, kart

kullanım gecikme cezası/faiz artışlarının müşteriye bildirimi ve faiz hesaplamaları, ücretlendirme, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri.

d) Finansal raporlama süreci: Banka kayıtlarının ve bilgi kaynaklarının finansal raporlamalarda kullanım sürecinin kontrolü, düzenleyici ve denetleyici otoritelere, sistemler aracılığıyla yapılan raporlamaların performans ve süreçlerinin kontrolü, düzenleyici ve denetleyici otoritelere, periyodik olarak gerçekleştirilen veri aktarımı ve süreçlerinin kontrolü, solo ve konsolide finansal raporların hazırlanması ve diğer süreç kontrolleri.

e) Ödeme sistemleri süreci: EFT, EMKT, Takasbank, SWIFT işlemleri ve bunlarla ilgili güvenlik kayıtları gibi ödeme sistemi kontrolleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri.

f) Hazine/Menkul kıymetler ve fon yönetimi süreci: Menkul kıymet ve fon yönetimi iş süreçlerinin kontrolü, limit tanımlamaları ve limitlerin takibi, nostro, vostro ve loro bakiyelere ilişkin mutabakatlar ve muhabir kayıtlarının kontrolü, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri.

(3) Kurum denetlenenlerde BSD kapsamında denetlenecek iş süreçlerini belirlemeye yetkilidir.

(4) İş süreçleri üzerindeki kontrollerin etkinliği, ilgili bilgi sistemleri genel kontrollerinin etkin ve yeterli olmasına bağlıdır. Bu nedenle denetçi, iş süreçleri üzerindeki kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin incelemelerde bulunurken, gerekli gördüğü bilgi sistemleri genel kontrollerinin etkinlik ve yeterlilik durumunu dikkate alır. Denetçi söz konusu genel kontrolleri, denetim kapsamına dâhil eder, etkinlik ve yeterlilikleri ile iş süreçleri üzerindeki kontrollere olan etkilerini değerlendirir.

(5) Denetçi ikinci fıkrada ifade edilen ve önemlilik değerlendirmesi sonucunda denetim kapsamına dâhil ettiği süreçler için asgari olarak aşağıdaki kontrolleri test eder:

a) Yönetimce kontrollerin etkin olarak çalışmasının engellenmesini önleyecek ya da tespit edecek kontroller.

b) Denetlenenin bilgi sistemleri genel kontrolleri ve iş süreçlerindeki kontrollere ilişkin risk değerlendirme süreci.

c) Süreç ve işlemlerin sonuçlarının gözetimine ilişkin gözden geçirme, raporlama, sorgulama ve mutabakat gibi kontroller.

ç) Kontrollerin gözetimine yönelik kontroller.

d) Bankalarda dönem sonuna ilişkin muhasebe ve finansal raporlama süreci üzerindeki kontroller.

e) Bankalarda mükerrer bilgi sistemleri ve çift kayıt sistemi gibi sahtecilik ve usulsüzlüklerin önlenmesine ve tespit edilmesine ilişkin kontroller.

f) Bankalarda faiz, masraf, komisyon, stopaj vs. oran ve miktarları, vade ve valör bilgileri ile diğer önem arz eden bankacılık bilgilerine ilişkin veri, işlem ve kayıtların bütünlüğü ve güvenilirliğine ilişkin kontroller.

g) Görevler ayrılığı prensibinin uygulanmasına ilişkin kontroller.

ğ) Yetkilendirme ve erişim kontrolleri ile bu kontrollerin gözden geçirilmesine ilişkin kontroller.

h) Risk arz eden işlemlerin gerçekleştirilmesinde yer alan/alması gereken onay mekanizmaları.

ı) Veri, işlem ve kayıtların gizliliğine ilişkin kontroller.

i) Denetim izlerinin tutulması, güvenliğinin sağlanması ve düzenli olarak gözden geçirilmesi ve değerlendirilmesine ilişkin kontroller.

İç kontrol ve iç denetim sistemine ilişkin değerlendirme

MADDE 26 – (1) Denetçi, bilgi sistemleri genel kontrolleri ve iş süreçleri üzerindeki kontrollerle sınırlı olmak üzere denetlenenin iç kontrol ve iç denetim sistemleri bünyesinde yürüttüğü çalışmalarını önemlilik kriteri çerçevesinde değerlendirir. Bu kapsamda;

a) İç kontrol sistemine ilişkin yürütülen faaliyetler incelenirken asgari olarak;

1) Kontrol ortamına ilişkin hususlar,

2) Yönetim tarafından etkin ve yeterli bir iç kontrol sisteminin tesis edilmesi, işletilmesi ve gözetimine ilişkin benimsenen yaklaşım ve uygulaması,

3) Denetlenenin tabi olduğu mevzuat uyarınca kurulan meslek birlikleri tarafından belirlenen etik ilkelerin uygulanması ve çalışanların bu konudaki farkındalık düzeyi,

dikkate alınır.

b) İç denetim biriminin iç kontrol sisteminin etkinlik, yeterlilik ve uyumluluğunun gözetimine ilişkin yürüttüğü faaliyetler ve performansını değerlendirir.

c) İç denetim biriminin değerlendirilmesi kapsamında denetlenenin bilgi sistemleri denetimi faaliyetleri dikkate alınır. Denetlenenin bilgi sistemleri denetimi fonksiyonu değerlendirilirken asgari olarak;

1) Ekibin organizasyon içerisindeki yeri ve bağımsızlığı,

2) Ekibi oluşturan personelin nitelik ve sayı açısından yeterliliği,

3) Planlanan ve gerçekleştirilen denetim çalışmaları,

4) Denetim sonuçlarının takibi,

incelenir.

ç) Denetçi, denetlenenin iç kontrol sistemine ilişkin risk değerlendirme sürecinde yürütülen faaliyetlerini ve performansını değerlendirir.

ALTINCI BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Metodolojisi

Denetim stratejisi ve denetim planı

MADDE 27 – (1) Yürütülecek denetim çalışması için, denetlenenin faaliyetlerinin bilgi sistemlerine bağlılık ve bilgi sistemlerinin karmaşıklık derecesi, ekonomik, finansal beklentiler ile bunların bilgi sistemleri ile ilişkileri ve iç sistemlerinin yeterliliği hakkındaki denetçi kanaatine bağlı olarak denetimin kapsamı, zamanlaması ve yönlendirilmesini düzenleyen ve denetim planının geliştirilmesinde esas oluşturacak bir BSD stratejisi oluşturulur.

(2) BSD stratejisi, denetimin kapsamı, denetim esnasında kullanılacak önemlilik değerlendirmesi, denetlenecek süreçlerde denetim süresince meydana gelebilecek önemli değişiklikler gibi konuları içerir.

(3) Denetçi, denetim riskini makul bir düzeye indirebilecek yeterli ve uygun denetim kanıtının elde edilmesi için BSD stratejisine uyumlu bir denetim planı oluşturur.

(4) BSD stratejisi ve planı oluşturulurken, iç kontrol ve iç denetim raporları, BSD raporları, denetlenen ve Kurum arasında gerçekleşen yazışmalar ile Kurum tarafından verilen talimatlar dikkate alınır.

(5) BSD planlaması yapılırken, denetlenenin sistem ve süreçlerini konu alan bir risk değerlendirmesi çalışması yapılır ve bu çalışmanın sonuçları önemlilik kriteri açısından değerlendirilir.

(6) BSD planı asgari olarak;

a) Denetim tekniklerinin türü, zamanlaması ve detay seviyesinin tanımını,

b) Önemli veya kayda değer kontrol eksikliği risklerinin değerlendirilmesinde kullanılan risk değerlendirme tekniklerinin türü, zamanlaması ve detay seviyesinin tanımını,

c) BSD faaliyetinde görev alacak ekip üyelerinin bireysel yetenek ve yeterliliklerini dikkate alarak, denetim ekibinin sevkine ve faaliyetlerinin gözetimine ilişkin planlamayı,

içerir.

(7) BSD stratejisi ve denetim planı, denetim sürecinde gerekli görüldüğü takdirde nedenleri ile birlikte belgelenerek güncellenir ve değiştirilir.

(8) Denetçi, denetimi planlarken, hata, suistimal ve yasa dışı fiillere ilişkin riskleri dikkate alır.

Denetim teknikleri ve kontrollerin test edilmesi

MADDE 28 – (1) Denetçi, denetim görüşünün oluşturulmasına makul güvence sağlayacak düzeyde yeterli ve uygun denetim kanıtlarını elde etmek için aşağıdaki denetim tekniklerinden hepsini ya da bir kısmını uygun zaman ve detay kapsamıyla kullanır:

a) Tetkik.

b) Gözlem.

c) Sorgulama.

ç) Yeniden uygulama.

d) Yeniden hesaplama.

e) Analitik prosedür.

(2) Denetçi, test edeceği kontrollerin kapsamını, önemlilik ilkesini gözeterek ve test edeceği kontrol kümesinin bilgi sistemleri ve iş süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin bütününün etkinliği, yeterliliği ve uyumluluğu hakkında kendisine makul bir güvence sağlayacak şekilde belirler.

(3) Bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin etkin, yeterli ve uyumlu olduğuna dair görüş verilebilmesi için, incelemeye tâbi tutulan tüm kontrollerin, tasarım ve işletiminin etkinlikleri ve uyumluluklarının test edilmesi gerekir.

(4) Denetçi, denetim riskini kabul edilebilir bir seviyeye indirmek için, test ettiği kontrol ile ilişkili önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde testlerini detaylandırır, örneklem hacmini genişletir ve kanıtlarının yeterlilik ve güvenilirlik seviyesini artırır.

(5) Denetçi kontrole ilişkin test kapsamını belirlerken ilgili kontrolün uygulanma sıklığı, faal olma durumu açısından güvenilen süre, kontrollerdeki sapma beklentisi gibi kontrol karakteristiklerini dikkate alır.

(6) Denetçi sadece bilgi toplama tekniğini kullanarak elde ettiği denetim kanıtıyla bir kontrolün etkinlik, yeterlilik ve uyumluluğuna ilişkin görüş oluşturamaz.

(7) Denetçi, bir kontrolü test ederken dikkate alacağı zaman boyutunu denetim döneminin bütününe ilişkin görüş oluşturacak şekilde belirler.

Denetim örneklemesi

MADDE 29 – (1) Denetim örneklemesi; denetim tekniklerinin, tüm kalemlerin seçilme şansı olacak şekilde denetime ilişkin bir anakitlenin yüzde 100'ünden daha azına uygulanmasını ifade eder. Denetim örneklemesi denetçiye, örneklemin alındığı toplam veri seti ile ilgili görüş oluşturulabilmesini teminen seçilen örneklemle ilgili denetim kanıtlarını elde etme ve değerlendirme olanağı sağlar. Denetim örneklemesinde, istatistiki ya da istatistiki olmayan yaklaşımlar kullanılabilir.

(2) Denetçi, denetim örneklemini oluştururken, denetim tekniğinin amacını ve örnekleme seçileceği anakitlenin niteliklerini göz önünde bulundurmak zorundadır.

(3) Denetçi, örneklem büyüklüğünü belirlerken, denetim riskinin kabul edilebilir düşük bir seviyeye indirilip indirilmediğini dikkate almak zorundadır. Örneklem büyüklüğü, denetçinin kabul edebileceği denetim riski seviyesinden etkilenir. Denetçinin kabul edebileceği risk düştükçe, örneklem büyüklüğünün de o oranda artması gerekir.

(4) Denetçi, anakitlede yer alan tüm örnekleme birimlerinin seçilme şansı olduğu beklentisiyle örnek seçimini yapar. Denetim örneklemesinin amacı anakitlenin tümüne ilişkin sonuçlar ortaya çıkarmak olduğundan, denetçi anakitleyi temsil edecek özelliklere sahip ve önyargılardan uzak örneklem seçmeye gayret eder.

Denetim kanıtı

MADDE 30 – (1) Denetim kanıtı, denetçinin bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin görüşünü dayandırdığı sonuçlara ulaşmak amacıyla kullandığı tüm bilgilerdir.

(2) Denetçi; görüşünü dayandırdığı yeterli ve uygun denetim kanıtlarını elde edebilmek için gerekli denetim prosedürlerini tasarlar ve gerçekleştirir.

(3) Test edilmek üzere seçilen her bir kontrolün; etkinlik ve yeterliliğine ilişkin gerekli denetim kanıtı seviyesi, ilgili kontrolün çalışmaması durumunda önemli veya kayda değer kontrol eksikliğine sebebiyet verme ihtimaline bağlıdır.

(4) Denetçinin, güvenilir denetim kanıtı elde edebilmesi için, uyguladığı denetim tekniklerinin dayandığı bilgilerin tam ve doğru olması gerekir. Denetçi, denetim tekniklerini uygularken tam ve doğru olduğuna ilişkin yeterli araştırmayı yapmak koşuluyla denetlenen tarafından üretilen bilgileri de kullanabilir.

Bulguların değerlendirilmesi

MADDE 31 – (1) Denetçi, denetim çalışmasının sonunda, tespit ettiği her bir kontrol zayıflığını ayrı ayrı inceler ve bu zayıflıkları hem tek başlarına, hem de birlikte oluşturacakları farklı kombinasyonlarla değerlendirerek bunların kayda değer kontrol eksikliği veya önemli kontrol eksikliği olarak sınıflandırılmasını nitel ve nicel yöntemler kullanarak gerçekleştirir.

(2) Denetçi, kontrol zayıflıklarını değerlendirirken temel olarak; bunların birlikte veya ayrı ayrı; sebep olabileceği yanlışlıkların ortaya çıkma olasılığını ve ortaya çıktığındaki etkisini göz önünde bulundurur.

(3) Denetçi, bilgi sistemleri genel kontrollerine ilişkin kontrol zayıflıklarını değerlendirirken, bunların iş süreçleri üzerindeki kontrollere olan etkisini de dikkate alır.

(4) Denetçi, denetim esnasında aşağıdaki alanlardan herhangi birinde kontrol zayıflığı ile karşılaşması durumunda bunları en azından kayda değer kontrol eksikliği olarak kabul eder:

a) Türkiye Muhasebe Standartlarının uygulanmasına ilişkin politikalar.

b) Denetlenenin tabi olduğu Kanun ve bu Kanunlara istinaden yayımlanan alt düzenlemeler ve talimatların gereğinin yerine getirilmesine ilişkin kontroller.

c) Sahteciliği önleyen kontroller veya programlar.

ç) Rutin veya sistematik olmayan işlemler.

d) Yılsonu finansal raporlama süreci.

(5) Denetçi aşağıdaki durumlardan herhangi biriyle karşılaşması halinde bunları en azından kayda değer kontrol eksikliği olarak kabul eder ve önemli kontrol eksikliğine güçlü birer işaret olarak algılar:

a) Hata veya suistimal nedeniyle, denetlenenin varlık ve yükümlülüklerinin farklı şekilde yansıtılarak mevzuatta tanımlanan ve yasal yükümlülükler bakımından denetlenen ile ilgili alınması gereken kararları veya sağlıklı bir finansal değerlendirme yapılmasını etkileyecek şekilde, önceden yayımlanmış olan finansal tablolar üzerinde düzeltmeler yapılması.

b) Cari döneme ait finansal tablolarda veya verilerde denetlenenin iç kontrol ve/veya iç denetim faaliyetleri sırasında önceden fark edilmemiş olan önemli bir yanlış beyanın denetim esnasında denetçi tarafından tespiti.

c) Denetlenenin farklı birimlerinden aynı hususa ilişkin olarak gelen bilgi, belge ve veriler arasında tutarsızlık olduğunun tespit edilmesi.

ç) Denetlenenin yönetimi tarafından denetçiye verilen beyanlarda kasıt içermese dahi önemli bir yanlış beyanın tespit edilmesi.

d) Aksiyon planında yer verilen taahhütlerin yerine getirilmemiş olması.

e) Bankanın büyüklüğü dikkate alınarak iç denetim ve risk yönetim fonksiyonlarının etkin bir iç kontrol ortamının tesis edilmesi için gerekli olduğunun düşünüldüğü durumlarda, bilgi sistemlerine yönelik söz konusu fonksiyonların bulunmaması veya etkin olmaması.

f) Bilgi sistemleri ile denetlenenin faaliyetlerine ilişkin süreç ve sistemler kapsamında mevzuata uyum kontrolünü sağlayacak bir birimin/fonksiyonun bulunmaması veya etkin olmaması.

g) Yönetici veya yöneticilerin dâhil olduğu küçük dahi olsa bir sahteciliğin tespit edilmesi.

ğ) Yöneticilere iletilmiş olan kayda değer bir kontrol eksikliğinin makul bir süre geçmesine rağmen hala düzeltilmemiş olması.

h) Etkin bir iç kontrol ortamının tesis edilmemiş olması.

ı) Bankalarda denetim komitesince, muhasebe, finansal raporlama ve iç kontrol sistemi üzerinde etkin bir gözetimin tesis edilmemiş olması.

(6) Denetçi bir önceki denetim döneminde tespit edilmiş ve devam eden bulguların cari dönemde de son durumlarını değerlendirerek raporlar.

Denetim görüşünün oluşturulması ve denetim mektubu

MADDE 32 – (1) Yapılan denetim sonucunda aşağıdaki durumlarda, kendilerine bağlı denetim ekiplerinin de görüşlerini alarak BSD gerçekleştiren kuruluşun BSD raporunu imzalamaya yetkili denetçileri bankalarda Ek-9, Risk Merkezi ve bilgi alışverişi kuruluşlarında Ek-17 ve diğer finansal kuruluşlarda Ek-21'de yer alan örneğe uygun olarak denetim mektubunda olumlu görüş bildirirler:

a) Herhangi bir önemli kontrol eksikliğinin bulunmaması.

b) Denetim kapsamında herhangi bir kısıtlama ya da engelleme ile karşılaşılmaması.

(2) Yapılan denetim sonucunda aşağıdaki durumlarda, kendilerine bağlı denetim ekiplerinin de görüşlerini alarak BSD gerçekleştiren kuruluşun BSD raporunu imzalamaya yetkili denetçileri bankalarda Ek-10, Risk Merkezi ve bilgi alışverişi kuruluşlarında Ek-18 ve diğer finansal kuruluşlarda Ek-22'de yer alan örneğe uygun olarak denetim mektubunda şartlı görüş bildirirler:

a) En az bir önemli kontrol eksikliğiyle karşılaşılmasına rağmen, bu eksikliklerin denetlenenin bilgi sistemleri ile iş süreç ve sistemlerinin bütününü veya büyük bir kısmını etkilemediğinin düşünülmesi.

b) Görüş bildirmekten kaçınmayı gerektirecek önemde olmamakla birlikte, BSD faaliyetlerini sınırlayan herhangi bir hususun varlığı veya yeni tesis edilmiş bir sistem veya süreç hakkında yeterince bilgi edinilememesi.

c) Denetim görüşünün oluşturulması için yeterli ve uygun denetim kanıtının elde edilememesi.

(3) Yapılan denetimlerde rastlanılan önemli kontrol eksikliklerinin tek başlarına veya beraber değerlendirilmeleri sonucunda bilgi sistemleri ile iş süreçlerinin bütününü veya büyük bir kısmını etkilediğine ilişkin kanaat edinilmesi durumunda, BSD gerçekleştiren kuruluşun BSD raporunu imzalamaya yetkili denetçileri kendilerine bağlı denetim ekiplerinin de görüşlerini alarak, bankalarda Ek-11, Risk Merkezi ve bilgi alışverişi kuruluşlarında Ek-19 ve diğer finansal kuruluşlarda Ek-23'te yer alan örneğe uygun olarak denetim mektubunda olumsuz görüş bildirirler.

(4) Denetim çalışmalarında karşılaşılan belirsizlik ve sınırlamaların görüş belirtilmesini engelleyecek derecede önemli olduğunu düşündükleri durumlarda, BSD gerçekleştiren kuruluşun BSD raporunu imzalamaya yetkili denetçileri kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, bilgi sistemleri ile iş süreçleri üzerindeki kontroller hakkında görüş bildirmekten kaçınabilirler. Görüş bildirmekten kaçınma durumunda düzenlenecek raporda, kaçınmaya yol açan nedenlere ilişkin denetçi görüşlerine yer verilmesi şarttır. Bu durumda bankalarda Ek-12, Risk Merkezi ve bilgi alışverişi kuruluşlarında Ek-20 ve diğer finansal kuruluşlarda Ek-24'te yer alan örneğe uygun olarak denetim mektubu düzenlenir.

(5) Bankalarda ve konsolidasyona tabi ortaklıklarında gerçekleştirilen BSD sonucunda 5 inci ve 7 nci maddelerde belirtilen hükümler ile bu maddede belirtilen görüş çeşitleri çerçevesinde; olumlu, şartlı veya olumsuz görüşe varılması hallerinde, sırasıyla Ek-13, Ek-14 ve Ek-15'te yer alan örneklere uygun olarak denetim mektubu düzenlenir. Görüş bildirmekten kaçınmayı gerektirecek şartların varlığı halinde ise, denetim mektubu Ek-16'da yer alan örneğe uygun olarak düzenlenir.

Denetim çalışmalarının belgelendirilmesi

MADDE 33 – (1) Denetçi; BSD raporunda yer vereceği görüşlerini desteklemek ve denetimin bu Yönetmelik hükümlerine uygun şekilde planlandığına ve gerçekleştirildiğine dair kanıt sunmak amacıyla denetimi gerçekleştirdiği süre zarfında çalışma kâğıtlarını hazırlar.

(2) Çalışma kâğıtları, toplanan kanıtların ve BSD raporunun nihai hale getirilmeden gözden geçirilmesine ve değerlendirilmesine imkân verecek şekilde hazırlanır.

(3) Denetçi, çalışma kâğıtlarını, yürütülen denetim çalışması ile hiçbir bağlantısı olmayan tecrübeli bir denetçinin;

a) Gerçekleştirilen denetimin bu Yönetmelikle belirlenen hükümlere uygunluğunu,

b) Toplanan denetim kanıtları ve uygulanan denetim tekniklerinin sonuçlarını,

c) Denetim sırasında ortaya çıkan önemli hususlar ve bunlarla ilgili ulaşılan değerlendirmeleri,

kavrayabilmesine olanak sağlayacak şekilde hazırlar.

(4) Çalışma kâğıtları fiziki veya elektronik ortamda tutulabilir.

(5) Çalışma kâğıtları üzerindeki tasarruf yetkisi denetçinin istihdam edildiği yetkili kuruluşa, BSD'nin dış hizmet alımı ile gerçekleştirilmesi halinde ise ilgili BDK'ya aittir. Çalışma kâğıtları, denetlenenin yazılı izni olmaksızın Kurum dışındaki üçüncü kişilere verilemez veya açıklanamaz. Çalışma kâğıtlarının gizliliğinin ve güvenliğinin sağlanması yetkili kuruluşun sorumluluğundadır.

(6) Yetkili kuruluş, BSD raporu tarihinden sonraki altmış gün içerisinde tüm çalışma kâğıtlarının bir araya getirilmesinden sorumludur. Çalışma kâğıtları BSD raporu tarihinden itibaren en az on yıl süreyle saklanır.

(7) Denetçi, çalışma kâğıtlarının nihai denetim dosyasında birleştirilmesi işlemi tamamlandıktan sonra mevcut çalışma kâğıtlarında değişiklik yapmayı veya yeni çalışma kâğıtları eklemeyi gerekli görürse, yapılan değişikliklerin veya eklemelerin niteliğine bakılmaksızın aşağıdaki hususları belgelendirir:

a) Değişiklik veya ekleme yapmasının özel sebepleri.

b) Değişiklik veya eklemelerin ne zaman ve kim tarafından yapıldığı ve gözden geçirildiği.

YEDİNCİ BÖLÜM
Genel İlkeler ve Sorumluluklar

BSD sözleşmesi

MADDE 34 – (1) BSD, yetkili kuruluş ile denetlenen arasında imzalanacak yazılı sözleşme çerçevesinde yürütülür. BSD sözleşmesi, yapılacak denetimin kapsam ve içeriği üzerinde taraflar arasında tam bir mutabakat sağlandığının göstergesidir.

(2) BSD sözleşmeleri, denetlenenin yönetim kurulunca onaylanarak yürürlüğe girer.

(3) Denetlenen, yetkili kuruluş ile aralarındaki BSD sözleşmesine ilişkin bilgileri, usul ve esasları Kurum tarafından belirlenecek şekilde, sözleşmenin imzalanmasını takip eden otuz gün içinde Kuruma ulaştırır.

(4) Yetkili kuruluş, denetlenen ile BSD sözleşmesi yapmadan önce BSD'nin kapsam ve planlamasını belirlemek amacıyla gerekli ön araştırmayı yapmak zorundadır. Ön araştırma kapsamında, denetim sürecini olumlu ya da olumsuz etkileyebilecek hususların varlığı ve yetkili kuruluş değişikliği halinde bunun nedenleri ile ilgili olarak önceki dönemlerde denetimi üstlenen yetkili kuruluşlardan bilgi talep edilebilir. Denetlenen, önceki yetkili kuruluşa cari dönem için sözleşme yaptığı yetkili kuruluşun unvanını bildirir ve talep edilen bilgilerin verilmesi için yetkilendirir. Önceki yetkili kuruluş, bu kapsamda kendilerinden talep edilen bilgileri vermek zorundadır.

(5) BSD sözleşmelerinde, asgari olarak aşağıdaki unsurların bulunması zorunludur:

a) Denetçinin uymakla yükümlü bulunduğu düzenlemeler.

b) BSD'nin amacı, kapsamı varsa özel nedenleri.

c) Yetkili kuruluş tarafından anlaşma kapsamında sunulacak hizmetler.

ç) Tarafların sorumluluk ve yükümlülükleri.

d) Denetimde görevlendirilecek denetçiler ile bunların yedekleri.

e) Denetim ekibinde görevlendirilenlerin unvanları, öngörülen çalışma süreleri ve her biri için uygun görülen ücret tutarının ayrıntılı dökümü.

f) Denetimin başlama ve bitiş tarihleri.

g) BSD raporunun ve istenmesi halinde özel amaçlı denetim raporunun şekli ve bu raporların hazırlanma nedenleri.

ğ) BSD raporunun teslim edileceği tarih.

(6) Denetçinin çalışma alanının önemli ölçüde sözleşme hükümlerine aykırı olarak sınırlandırılması, bilgi sistemleri ve iş süreçlerine ilişkin bilgi ve belgelerin elde edilememesi veya benzeri durumların oluşması halinde sözleşme, yazılı gerekçe göstermek ve Kuruma önceden bildirimde bulunulmuş olması koşuluyla, yetkili kuruluş tarafından feshedilebilir. Yetkili kuruluş bu durumu, denetimden çekilme gerekçeleriyle birlikte derhal Kuruma bildirir. Çekilen yetkili kuruluş çalışma kâğıtlarını ve gerekli tüm bilgileri, yerine geçecek olan yetkili kuruluşun incelemesine imkân sağlamak ve istenilmesi halinde bu dokümanlara ait uygun kopyaları sağlamakla yükümlüdür. Çekilen yetkili kuruluşun yerine geçecek yetkili kuruluşun Kurum tarafından uygun görülmesi şarttır.

(7) Denetçi, denetlenenin bazı faaliyetlerini BSDDHK aracılığı ile yürütmesi halinde BSD sözleşmesinde, BSDDHK bünyesinde bağımsız denetim yapılabilmesini temin eden hükümler bulunmasını sağlar.

(8) Sözleşmede, denetim hizmeti dışında başka bir hizmet yapılması öngörülemez.

SEKİZİNCİ BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetiminde İş Birliği

Başka taraflarca yapılan çalışmalardan yararlanma ve iş birliği

MADDE 35 – (1) Denetçi, görüşüne dayanak teşkil edecek temel kanıtları edinmek için yeterli çalışmayı bizzat gerçekleştirir. Bununla birlikte denetim çalışmasının yapı, zamanlama ve detay seviyesi açılarından genişletilmesi amacıyla diğer yetkili kuruluşların, denetlenenin iç sistemler birimlerinin ve uzman şahısların çalışmalarından yararlanabilir.

(2) Başka taraflarca gerçekleştirilen çalışmalardan yararlanmak, denetçinin denetime ilişkin sorumluluğunu azaltmaz. Denetçi, yararlandığı çalışmalara raporunda referans verebilir ve bu hususların güncel durumunu değerlendirerek rapora konu eder.

(3) Denetçi, denetim çalışmasında, denetlenenin iç sistemlerinin yeterliliği ve bağımsızlığı hakkındaki kanaatine bağlı olarak, denetlenenin iç denetim ve iç kontrol faaliyetlerini göz önünde bulundurarak mümkün olduğunca tekrardan kaçınmaya özen gösterir.

(4) Bilgi Sistemleri Bağımsız Başdenetçisi, başka taraflarca gerçekleştirilen çalışmalardan hangi detay seviyesinde yararlanılabileceğinin tespiti için asgari olarak;

a) Çalışmanın kapsamının uygunluğu ve denetim programının yeterliliğini,

b) İncelenen kontrollerin yapısını,

c) Çalışmayı gerçekleştiren şahısların mesleki yeterlilik, özen, tarafsızlık ve bağımsızlığını,

ç) Çalışmanın genelini değerlendirmeye yetecek kadarını test etmek suretiyle kalitesini,

değerlendirir.

(5) Önceki BSD'yi gerçekleştiren yetkili kuruluş ve denetçi, denetimine esas teşkil eden her türlü bilgi ve belgeyi gizlilik ilkesi çerçevesinde, BSD'yi yapacak yetkili kuruluş ve kişilere sağlamakla yükümlüdür.

(6) Denetlenenin iç denetçileri ve iç kontrol faaliyetlerinden sorumlu olanlar, kendi raporları dâhil ihtiyaç duyulan bütün bilgileri denetçilere vermekle yükümlüdürler.

Kurum ve yetkili kuruluşlar arası iş birliği

MADDE 36 – (1) Kurum personeli, yetkili kuruluşların BSD sürecinin her aşamasına, bilgi ve becerilerini geliştirmek amacıyla, denetçi bağımsızlığı ilkesini zedelemeksizin izleyici sıfatı ile eşlik edebilir. Kurum personeli, yetkili kuruluşun bilgi birikimini şahsına veya bir başka yetkili kuruluşa çıkar sağlamak için kullanamaz. Yetkili kuruluş, Kurum personelinin süreçte yer alması ve bilgi birikimini artırması bakımından gerekli katkı ve çabayı gösterir.

(2) Yetkili kuruluş birinci fıkra hükümlerinin uygulanmasına yönelik olarak denetlenendeki denetim programını, Kurumun talebine bağlı olarak, denetim çalışmalarının fiilen başlamasından önce Kuruma bildirir.

Dış hizmet sağlayıcıların denetlenmesi

MADDE 37 – (1) Denetçi, denetlenenin dış hizmet sağlayıcı kuruluşlar ile gerçekleştirdiği hizmetlerin bilgi sistemlerini ve iş süreçlerini nasıl etkilediğini göz önünde bulundurur, denetimini buna göre planlar ve etkin bir denetim yaklaşımı geliştirir.

(2) Denetçi, dış hizmet sağlayıcının, sunduğu hizmete ilişkin sahip olduğu, güncelliğini yitirmemiş denetim raporu, sertifika gibi belgelerden 35 inci madde kapsamında faydalanabilir.

(3) Dış hizmet sağlayıcı için hazırlanan güvence raporunun bu Yönetmelik kapsamında kullanılabilmesi/geçerli olabilmesi için güvence raporunun;

a) Bu Yönetmelik kapsamında yetkilendirilmiş bir BDK tarafından hazırlanmış olması,

b) Dış hizmet sağlayıcının denetlenene verdiği hizmetlerin tamamını kapsaması,

c) Denetlenenin tabi olduğu mevzuata göre, bu Yönetmelik kapsamında düzenlenmiş olması,

gerekmektedir.

DOKUZUNCU BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Raporu ve Bildirimi

BSD raporu

MADDE 38 – (1) BSD raporu, önemlilik kavramı da dikkate alınarak, bilgi sistemleri ve iş süreçleri üzerinde değerlendirmelere yer verilen ve denetçinin kanaatinin net bir dille yazılı olarak açıklandığı metindir. Denetçinin görevi, bilgi sistemleri ve iş süreçleri üzerindeki kontroller hakkında denetim kanıtlarını toplayıp incelemek, değerlendirmek ve bu kanıtlar üzerinde bir sonuca ulaşarak denetim hakkında kanaat oluşturmaktır.

(2) Denetçi, BSD raporunu denetim çalışmaları sonrasında denetimin gerçekleştirildiği döneme ait faaliyetlerin tamamını kapsayacak şekilde düzenlemek zorundadır. Rapora ilişkin usul ve esaslar Kurul tarafından düzenlenir.

(3) Düzenlenen BSD raporları, Kurum tarafından aksi belirtilmedikçe, ilgili kuruluşun bağımsız denetim raporuyla birlikte tamamlanır.

(4) BSD raporları Bankalarda, Risk Merkezi ve bilgi alışverişi kuruluşlarında denetimden sorumlu Bilgi Sistemleri Bağımsız Başdenetçisi ile yetkili kuruluşun BBDY'nin 3 üncü maddesinde tanımlanan sorumlu denetçisi, diğer finansal kuruluşlarda Bilgi Sistemleri Bağımsız Başdenetçisi tarafından imzalanır.

(5) Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında yapılan denetim sonucu düzenlenen BSD raporu, yetkili kuruluşu temsil ve ilzama yetkili olanların imzasını taşıyan bir yazı ekinde denetlenenin yönetim kuruluna, bankalarda ayrıca denetim komitesine ve Risk Merkezi'nde Risk Merkezi yönetimine iletilir.

(6) Diğer finansal kuruluşlarda yapılan denetim sonucu düzenlenen BSD raporu yetkili kuruluşu temsil ve ilzama yetkili olanların imzasını taşıyan bir yazı ekinde denetlenenin yönetim kurulu başkanlığına iletilir.

(7) BSD raporunun içeriği gizli bilgi niteliği taşır ve herhangi bir ortamda yayımlanmaz. Bu bilgilerin gizliliği ve güvenliği, Kurumun, yetkili kuruluşların, BSDDHK'ların ve denetlenenin sorumluluğundadır. Denetlenenler, denetim sonuçlarını içerecek beyanatlar veremezler ve bu hususları reklam amaçlı kullanamazlar.

(8) BSD raporları Kurumca belirlenecek usul ve esaslar kapsamında Kuruma raporlanır.

ONUNCU BÖLÜM
Bilgi Sistemleri Bağımsız Denetim Sicili

Sicile kayıt

MADDE 39 – (1) Kurum tarafından BSD yapma yetkisine sahip olan kuruluşa ve 18 inci madde kapsamında Bilgi Sistemleri Bağımsız Başdenetçisi unvanı sahip olan denetçiye bir sicil numarası verilir.

(2) BSD yapma yetkisinin geçici veya sürekli olarak kaldırılması, uyarı, idari para cezası işlemleri Kurumca elektronik ortamda tutulan sicile kaydedilir.

Sicil bilgileri

MADDE 40 – (1) Kurumca tutulan sicilde yetkili kuruluşların;

a) Ticaret unvanı ve ticaret sicil numarası,

b) Kurum tarafından verilen sicil numarası,

c) Merkez adresi ve varsa şube adresleri (varsa, bünyesinde bulunduğu denetim ağı ve bu ağın hukuki ve yapısal niteliği, ilişkili denetim kuruluşu ve diğer işletmeleri ve bu kuruluşun hukuki ve yapısal niteliği),

ç) İnternet sitesi adresi,

d) Ortaklarının ad ve soyadları, T.C. kimlik numaraları ve şirket sermayesindeki payları, pay oranları ve tutarları,

e) Gerçekleştirilen BSD listesi,

f) Denetçilerinin listesi ve sicil numaraları,

g) Kurumca gerekli görülen diğer bilgileri,

kaydedilerek takibi yapılır.

(2) Kurumca tutulan sicilde denetçilerin;

a) Adı soyadı, T.C. kimlik numarası,

b) Kurum tarafından verilen sicil numarası,

c) İletişim bilgileri,

ç) Ortak olduğu veya istihdam edildiği denetim kuruluşuna ait ticaret unvanı, ticaret sicil numarası, varsa internet sitesi adresi ve iletişim bilgileri,

d) Sorumlu Bilgi Sistemleri Başdenetçisi olarak gerçekleştirdiği BSD'leri,

e) Kurumca gerekli görülen diğer bilgileri,

kaydedilerek takibi yapılır.

(3) Kurum sicile kaydedilen denetçi ya da yetkili kuruluşa ilişkin bilgilerin uygun gördüklerini Kurum internet sayfasında yayımlamaya yetkilidir.

ON BİRİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Denetçilerin denetlenenler bünyesinde görev almaları

MADDE 41 – (1) Bilgi Sistemleri Bağımsız Başdenetçileri, son iki yıl içinde denetim sürecine katıldıkları denetlenenlerde ve bağlı ortaklıklarında görev alamazlar.

Yönetmelikte hüküm bulunmayan haller

MADDE 42 – (1) Bu Yönetmelikte hüküm bulunmayan hallerde Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından yayımlanan;

a) BDS 300 Finansal Tabloların Bağımsız Denetiminin Planlanması Standardının, denetim stratejisi ve denetim planı,

b) BDS 402 Hizmet Kuruluşu Kullanan Bir İşletmenin Bağımsız Denetiminde Dikkate Alınacak Hususlar Standardının, dış hizmet sağlayıcıların denetlenmesi,

c) BDS 500 Bağımsız Denetim Kanıtları Standardının, denetim kanıtı,

ç) BDS 530 Bağımsız Denetimde Örnekleme Standardının, denetim örneklemesi,

ile ilgili paragrafları bilgi sistemleri bağımsız denetimine kıyasen uygulanır.

Yürürlükten kaldırılan yönetmelik

MADDE 43 – (1) 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik yürürlükten kaldırılmıştır.

(2) Birinci fıkra ile yürürlükten kaldırılan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliğe yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Yürürlük

MADDE 44 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 45 – (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

Ekleri için tıklayınız.